Application Service Provider Privacy & Security Policies

Access	Sage Intergy On-Demand uses standard, browser based technology. It is hosted at a data center and made available via thin client such as Terminal Services or Citrix Windows(r) XP (or higher) operating system and Internet Explorer, or similar commercially available web browser are used to access the system. Since access to and performance of the Sage Intergy On-Demand solution is directly related to the bandwidth (or speed) and availability of an internet connection, it is vital that the practice has a quality internet connection with a reliable local Internet Service Provider (ISP). The internet connection must meet an estimated 64 kbps download speed and 28 kbps upload speed per concurrent user bandwidth requirement (with additional bandwidth required for scanning of 128 kbps download speed and 192 kbps upload speed per scanner) to ensure speedy access to Sage Intergy On-Demand. Workstation Specifications - Windows XP SP2 operating system, 850 MHz Pentium processor or equivalent, 512 MB RAM (Minimum), SXGA video, Internet Explorer 6.0 or higher. Other Software: Microsoft Remote Desktop Client 5.2 or higher, Java Runtime Environment 1.50.14 or higher, and Adobe Acrobat Reader 8.12 or higher.
Authorization	Sage requires each Provider License and User to have a user name and password at two levels; a first level to access the hosted server and a second level to access the Sage Intergy On-Demand application. The first level access to the hosted server requires the user's names to be recorded at our datacenter and the second level access to the Sage Intergy On-Demand application is managed by a member of management at the practice. In addition, the Sage Intergy On-Demand application requires setup for each user to clarify what parts of the application the user may enter and use. Passwords are controlled by the customer
Authentication	Secure Communications - All information transmitted into and out of the data center is encrypted with state of the art 128-bit SSL encryption. Secure Servers - All systems protected from intruders, including hackers, viruses, spam, and other malware. Protection mechanisms are constantly maintained and updated to insure systems are protected from the latest threats.
Audit	The dedicated Sage Intergy On-Demand servers are hosted in a triple secure network with 128-bit SSL encryption (providing complete data protection from spam, viruses, and malware), are fireproof, and located in a climate-controlled data center that uses state-of-the-art technology for continual monitoring - 24 hours a day, 7 days a week, 365 days a year. Other features of the facilities include: * SunGard/Vericenter Datacenters, SAS 70 Type II Compliant

	* Multiple redundant connections to the internet backbone to accommodate high-traffic volumes. Systems will automatically select the fastest way to move data and will even seamlessly switch to another internet carrier if one provider goes down. * Uninterrupted Power Supply (UPS) deployed in a parallel redundant configuration, with a two-megawatt generator backup available in the event of a utility failure. * 24/7 security, including centralized security stations, closed-circuit digital camera monitoring and recording, and biometric palm scanners and proximity card readers that control access to the facility. * Advanced fire-suppression detection using a VESDA (Very Early Smoke Detection Apparatus) air sampling system. * Data-grade heating, venting, and air conditioning (HVAC) system. * 24/7 advanced critical systems monitoring and disaster prevention of all facility systems.
Secondary Uses of Data	None at this time.
Data Ownership	The client owns the data, but not the hosted server or application.